

CVE-2025-61810

ColdFusion versions 2025.4, 2023.16, 2021.22 and earlier are affected by a Deserialization of Untrusted Data vulnerability that could result in arbitrary code execution in the context of the current user. A high privileged attacker could exploit this vulnerability by providing maliciously crafted serialized data to the application. Exploitation of this issue requires user interaction and scope is changed.

EVRS 16 /100 Elevated priority	CVSS V3.1 8.4 High · NVD	EPSS 0.095 95.5th percentile · FIRST	CISA DEADLINE — No CISA deadline
---	--	--	--

Signals behind the score

☒ counted in the score ☐ not counted evidence for 3 of 8 signals

☐ CISA KEV	Not currently CISA KEV-listed	☐ Vendor exploitation	Active-exploitation status not yet checked - scored at the population base rate (none) until known
☐ Ransomware	Ransomware association unavailable	☐ KEV recency	CISA KEV listing date unavailable
☒ EPSS	0.095 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.4	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Scheduled Maintenance Patch or fixed version identified

Apply the vendor patch or guidance: <https://github.com/advisories/GHSA-cjmh-96m9-g6qr> | <https://helpx.adobe.com/security/products/coldfusion/apsb25-105.html>

Basis: External remediation intelligence

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
coldfusion	2021 2023 2025	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-cjmh-96m9-g6qr	Additional guidance	helpx.adobe.com/security/products/coldfusion/apsb25-105.html
NVD	nvd.nist.gov/vuln/detail/CVE-2025-61810	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2025-202344
Current data	evulnable.com/vulnerability-management/cve/CVE-2025-61810		

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.